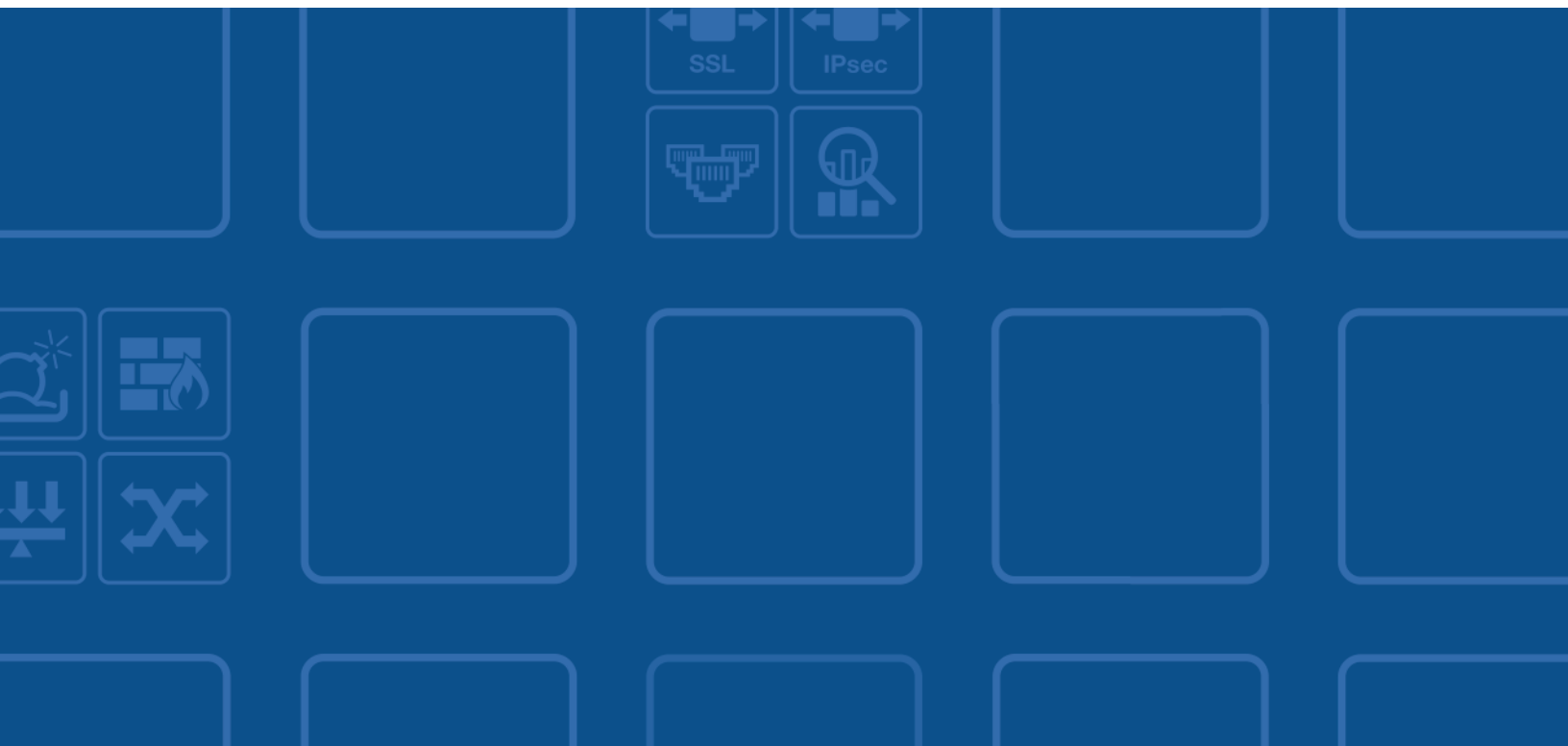
FORTINET
High Performance Network Security

FortiAnalyzer - XML API Reference

VERSION 5.4.1



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

June 29, 2016

FortiAnalyzer 5.4.1 XML API Reference

05-541-309862-20160629

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-02-17	Initial release
2016-06-29	Updated for FortiAnalyzer 5.4.1.

Introduction

FortiAnalyzer 5.4 includes a web service interface that facilitates integration with provision systems.

This guide describes how to use the XML-based FortiAnalyzer Application Programming Interface (API) to obtain information from the FortiAnalyzer unit, run scripts to modify device configurations, and install modified configurations to managed devices.

What’s New in FortiAnalyzer 5.4

What's New in FortiAnalyzer 5.4.1

The *vdom* element has been added to the *getFazArchive* and *removeFazArchive* commands.

Using the FortiAnalyzer API

The FortiAnalyzer enables you to configure managed FortiGate devices through a web service interface.

This sections includes the following topics:

Connecting to FortiAnalyzer web service

Enabling web service

Web service must be enabled on the network interface that the client will connect to.

To enable web service on an interface with the GUI:

1. Go to *System Settings* > *Network* > *All Interfaces*.
2. Select an interface, and click *Edit*.

3. In the *Administrative Access* section, select *Web Service*.
4. Select *OK* to apply the changes.

To enable web service on an interface using the CLI:

Enter the following command line interface (CLI) commands:

```
config system interface
     edit <port>
        set allowaccess webservice
     end
  end
```

where `<port>` is the network interface that you want to use for web service.

The `allowaccess` command should also include the other types of administrative access that you want to permit. For example, to allow HTTPS, SSH, and Web Service, enter the CLI command `set allowaccess https ssh webservice`.

The FortiAnalyzer unit handles web service requests on port 8080.

Obtaining the WSDL file

You can download a WSDL file for legacy operations or for new operations.

By using a web testing tool, such as SoapUI, you can get information from your FortiAnalyzer.

WSDL file for legacy operations

This section describes how to download a WSDL file by using the GUI. You can also use the CLI to download the WSDL file directly from your FortiAnalyzer at the following URL:

https://<FortiAnalyzer_ip_address>:8080/

To download the WSDL file using the GUI:

1. Go to *System Settings* > *Advanced* > *Advanced Settings*.
2. In the *Download WSDL file* section, select *Legacy Operations*, and then click *Download*.
3. Save the `xml.wsdl` file to your local hard disk drive. You can open this file using a text editor.

WSDL file for new operations

This section describes how to download a WSDL file by using the GUI. You can choose to download one or both of the new modules in a WSDL file.

To download the WSDL file using the GUI:

1. Go to *System Settings* > *Advanced* > *Advanced Settings*.
2. In the *Download WSDL file* section, select one or both of the following modules, and then click *Download*:

- *CLI Configuration*
- *System Commands*

3. Save the `xml.wsdl` file to your local hard disk drive. You can open this file using a text editor.

Getting information from the FortiAnalyzer unit

To work with your managed devices, you need to obtain information from your FortiAnalyzer unit, such as:

- A list of ADOMs
- Information about the managed devices
- Information about individual devices
- The current configuration of devices, according to the database
- The revision history of devices.

SOAP error codes and descriptions

- SOAP_ERROR_OK = 0, /* same with SOAP_OK */
- SOAP_ERROR_DEFAUT_ZONE = -100, /* This is obsoleted */
- SOAP_ERROR_INVALID_PARAM = -101, /* invalid parameter(s) */
- SOAP_ERROR_PREPARE_PROBLEM = -102, /* prepare problem(s) */
- SOAP_ERROR_NOT_SUPPORTED = -103, /* not supported */
- SOAP_ERROR_FUNC_PROBLEM = -104, /* function problem */
- SOAP_ERROR_WRONG_CONDITION = -105, /* wrong condition(s) */
- SOAP_ERROR_MEMORY_LIMIT = -106, /* not enough memory */

Besides the *errorMsg* response, there could be errors returned in `<SOAP-ENV:Fault>` envelope as well. These are considered generic SOAP errors. There are also cases in which errors from the FortiAnalyzer application level are returned inside `<SOAP-ENV:Fault>` envelope. These errors are free-style; there are no error codes associated with them.

For example:

```
<SOAP-ENV:Fault>
   <faultcode>SOAP-ENV:Client</faultcode>
   <faultstring>Invalid admin uesr name '(null)'</faultstring>
   <detail>
   <error xmlns="http://localhost/">Invalid admin user name '(null)'</error>
   </detail>
</SOAP-ENV:Fault>
```

FortiAnalyzer Legacy XML API elements

addAdom

Use this request to add an ADOM to your FortiManager unit.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:addAdom>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>?</userID>
         <!--Optional:-->
         <!--type: string-->
         <password>?</password>
      </servicePass>
      <!--type: string-->
      <name>?</name>
      <!--type: int-->
      <version>?</version>
      <!--type: int-->
      <mr>?</mr>
      <!--Optional:-->
      <!--type: boolean-->
      <isBackupMode>?</isBackupMode>
      <!--Optional:-->
      <!--type: boolean-->
      <VPNManagement>?</VPNManagement>
      <!--Zero or more repetitions:-->
      <deviceSNVdom>
         <!--Optional:-->
         <!--type: string-->
         <SN>?</SN>
         <!--Zero or more repetitions:-->
         <!--type: string-->
         <vdomName>?</vdomName>
         <!--Zero or more repetitions:-->
         <!--type: unsignedLong-->
         <vdomID>?</vdomID>
      </deviceSNVdom>
      <!--Zero or more repetitions:-->
      <deviceIDVdom>
         <!--Optional:-->
         <!--type: unsignedLong-->
         <ID>?</ID>
         <!--Zero or more repetitions:-->
         <!--type: string-->
         <vdomName>?</vdomName>
```

```
            <!--Zero or more repetitions:-->
            <!--type: unsignedLong-->
            <vdomID>?</vdomID>
         </deviceIDVdom>
      </r20:addAdom>
   </soapenv:Body>
```

Request Field	Description
<servicepass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<name>	The name of the ADOM to be created.
<version>	Firmware version options: • `400`: FortiOS version 4.0. • `500`: FortiOS version 5.0.
<mr>	The firmware major release version.
<isBackupMode>	Backup Mode ADOM options: • true: `BackupMode` is enabled. • false: `BackupMode` is disabled.
<VPNManagement>	VPN console ADOM options: • true: VPN console is enabled. • false: VPN console is disabled.
<deviceSNVdom>	XML structure consists of serial number, VDOM name, and VDOM ID variables.
<SN>	Serial number of device.
<vdomName>	The name of the VDOM.
<vdomID>	The VDOM identifier.
<deviceIDVdom>	XML structure consists of device ID, VDOM name, and `VDOM identifier` variables.
<ID>	The VDOM ID.
<vdomName>	The name of the VDOM.
<vdomID>	The VDOM identifier.

The response indicates if the request was successful or if it failed.

Example request:

```
soapenv:Header/>
<soapenv:Body>
   <r20:addAdom>
      <servicePass>
         <userID>admin</userID>
         <password></password>
      </servicePass>
      <name>NewADOM</name>
      <version>500</version>
      <mr>2</mr>
   </r20:addAdom>
</soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:addAdomResponse>
         <errorMsg>
            <errorCode>0</errorCode>
            <errorMsg>ADOM NewADOM added successfully</errorMsg>
         </errorMsg>
   </ns3:addAdomResponse>
</SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and details.
<errorCode> <errorMsg>	Error code and message details: • 0: Added members to the ADOM successfully. • -101: The user does not have permission to run this command. Cannot get ADOM OID. • -102: The global workspace is locked. Cannot get ADOM detail information. • -104: Cannot get ADOM detail information. • -106: Not enough memory.

addDevice

Use this request to add a device to your FortiManager unit.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:addDevice>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
```

```
            <!--type: string-->
            <userID>?</userID>
            <!--Optional:-->
            <!--type: string-->
            <password>?</password>
         </servicePass>
         <!--Optional:-->
         <!--type: string-->
         <adom>?</adom>
         <!--Optional:-->
         <!--type: string-->
         <ip>?</ip>
         <!--Optional:-->
         <!--type: string-->
         <autod>?</autod>
         <!--Optional:-->
         <!--type: string-->
         <deviceType>?</deviceType>
         <!--Optional:-->
         <!--type: string-->
         <name>?</name>
         <!--Optional:-->
         <!--type: string-->
         <adminUser>?</adminUser>
         <!--Optional:-->
         <!--type: string-->
         <password>?</password>
         <!--Optional:-->
         <!--type: int-->
         <version>?</version>
         <!--Optional:-->
         <!--type: int-->
         <mr>?</mr>
         <!--Optional:-->
         <!--type: string-->
         <model>?</model>
         <!--Optional:-->
         <!--type: string-->
         <flags>?</flags>
         <!--Optional:-->
         <!--type: string-->
         <description>?</description>
         <!--Optional:-->
         <!--type: string-->
         <devId>?</devId>
         <!--Optional:-->
         <!--type: string-->
         <SN>?</SN>
         <!--Optional:-->
         <!--type: string-->
         <SNprefix>?</SNprefix>
         <!--Optional:-->
         <!--type: boolean-->
         <forceProbe>?</forceProbe>
      </r20:addDevice>
   </soapenv:Body>
   </soapenv:Envelope>
```

Request Field	Description
<servicepass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<adom>	If the ADOM field is blank, the default ADOM will be that of the administrative user. If this administrator binds to all ADOMs, then the ADOM is root.
<ip>	The device IP address.
<autod>	autod options: `true`, `false`, `manual`, or `unreg` Select if you want to enable auto discovery. The default value is `False`. Select the value `unreg` to promote an unregistered device.
<deviceType>	Select the type of device. The device type can be: FortiGate, FortiCarrier, or FortiSwitch.
<name>	The host name of the device.
<adminUser>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<version>	Firmware version options: • `400`: FortiOS version 4.0. • `500`: FortiOS version 5.0.
<mr>	The firmware major release version.
<model>	The device model number, FGT-60C, for example.
<flags>	Flags options: • harddisk: The device has a hard disk installed. • No value: Leave this field blank if the device does not have a hard disk installed.
<description>	The device description (optional).
<devId>	The device identifier.
<SN>	The device serial number.
<SNprefix>	The device serial number prefix.
<forceProbe>	

The response is a series of <return> tags, each containing information about the device.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:addDevice>
      <servicePass>
         <userID>admin</userID>
         <password></password>
      </servicePass>
      <adom>FMGadom</adom>
      <ip>1.1.1.225</ip>
      <autod>true</autod>
      <deviceType>FortiManager</deviceType>
      <name>FMG</name>
      <adminUser>admin</adminUser>
      <password></password>
      <version>500</version>
      <mr>2</mr>
      <model>FMG-VM64</model>
      <flags></flags>
      <description>An FMG</description>
      <devId>FMG</devId>
      <SN>FMG-VM0000000000</SN>
      <forceProbe>true</forceProbe>
   </r20:addDevice>
</soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:addDeviceResponse>
         <errorMsg>
            <errorCode>0</errorCode>
            <errorMsg>Read task ID 10 to get addDevice result</errorMsg>
         </errorMsg>
         <taskId>10</taskId>
   </ns3:addDeviceResponse>
</SOAP-ENV:Body>
```

Response Field	Description
<errormsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.

Response Field	Description
<errorCode>	Error code and message details: • 0: Read task ID to get add device result. • -101: The device IP cannot be empty. The device name must be input. Administrator user must be input. Unknown device type; only accepts `FortiGate`, `FortiCarrier`, or `FortiSwitch`. The device firmware version (400, or 500) must be input. The device version should be 400 or 500 value is invalid. The device version mr (0, 1, etc...) must be input. The device version major release is invalid. The device model (FortiGate-200B, FortiWiFi-60C, etc...) must be input. The device model is invalid. The device ID must be set when promoting an unregistered device. Promotable device does not exist. The device is not an unregistered device. • -102: The ADOM is locked. • -103: Add device auto discovery mode is not supported yet. • -104: Add device by IP in ADOM failed. Promote device by device ID in ADOM failed.
<errorMsg>	
<taskid>	Indicates the task ID number.

deleteAdom

Use this request to delete an ADOM from your FortiManager unit.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:deleteAdom>
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>?</userID>
         <!--Optional:-->
         <!--type: string-->
         <password>?</password>
      </servicePass>
      <!--Optional:-->
      <!--type: string-->
      <adomName>?</adomName>
      <!--Optional:-->
      <!--type: string-->
      <adomOid>?</adomOid>
   </r20:deleteAdom>
</soapenv:Body>
```

Request Field	Description
<servicepass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<adomName>	The name of the ADOM.
<adomOid>	The ADOM object identifier (OID).

The response indicates with the request was successful or if it failed.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:deleteAdom>
      <servicePass>
         <userID>admin</userID>
         <password></password>
      </servicePass>
      <adomName>NewADOM</adomName>
   </r20:deleteAdom>
</soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:deleteAdomResponse>
         <errorMsg>
            <errorCode>0</errorCode>
            <errorMsg>Delete adom ID 129 successfully</errorMsg>
         </errorMsg>
   </ns3:deleteAdomResponse>
</SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • 0: Deleted ADOM ID successfully. • -101: The ADOM name is invalid. Cannot get a valid ADOM ID. Invalid ADOM. • -102: The ADOM is locked. The global workspace is locked. • -104: The ADOM ID cannot be deleted. • -105: The root ADOM cannot be deleted. The ADOM ID is in use and cannot be deleted.
<errorMsg>	

deleteDevice

Use this request to delete a device defined on your FortiManager unit.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:deleteDevice>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>?</userID>
         <!--Optional:-->
         <!--type: string-->
         <password>?</password>
      </servicePass>
      <!--Optional:-->
      <!--type: string-->
      <devId>?</devId>
      <!--Optional:-->
      <!--type: string-->
      <serialNumber>FGT60C3G06500185</serialNumber>
   </r20:deleteDevice>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<devId>	The device ID number.
<serialNumber>	The serial number of device.

The response indicates if the device was deleted successfully or if the procedure failed.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:deleteDevice>
      <servicePass>
         <userID>admin</userID>
         <password></password>
      </servicePass>
      <devId>467891</devId>
      <serialNumber>FGT60C0000000000</serialNumber>
   </r20:deleteDevice>
```

```
</soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:deleteDeviceResponse>
         <errorMsg>
            <errorCode>0</errorCode>
            <errorMsg>Delete device ID 467891 successfully</errorMsg>
         </errorMsg>
   </ns3:deleteDeviceResponse>
</SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode> <errorMsg>	Error code and message details: • 0: Read task ID to get delete device result. • -102: The ADOM is locked. • -104: The device can only be deleted from the ADOM which contains its root VDOM. The device ID cannot be deleted. • -105: The device ID is in use and cannot be deleted. The device ID was locked and cannot be deleted.

editAdom

Use this request to edit an ADOM.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:editAdom>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>?</userID>
         <!--Optional:-->
         <!--type: string-->
         <password>?</password>
      </servicePass>
      <!--type: string-->
      <name>?</name>
      <!--Optional:-->
      <!--type: int-->
      <version>?</version>
      <!--Optional:-->
      <!--type: int-->
      <mr>?</mr>
```

```
        <!--Optional:-->
        <!--type: boolean-->
        <state>?</state>
        <!--Optional:-->
        <!--type: boolean-->
        <isBackupMode>?</isBackupMode>
        <!--Optional:-->
        <!--type: boolean-->
        <VPNManagement>?</VPNManagement>
        <!--Optional:-->
        <metafields>
           <!--Zero or more repetitions:-->
           <metafield>
              <!--type: string-->
              <name>?</name>
              <!--type: string-->
              <value>?</value>
           </metafield>
        </metafields>
        <!--Zero or more repetitions:-->
        <addDeviceSNVdom>
           <!--Optional:-->
           <!--type: string-->
           <SN>?</SN>
           <!--Zero or more repetitions:-->
           <!--type: string-->
           <vdomName>?</vdomName>
           <!--Zero or more repetitions:-->
           <!--type: unsignedLong-->
           <vdomID>?</vdomID>
        </addDeviceSNVdom>
        <!--Zero or more repetitions:-->
        <addDeviceIDVdom>
           <!--Optional:-->
           <!--type: unsignedLong-->
           <ID>?</ID>
           <!--Zero or more repetitions:-->
           <!--type: string-->
           <vdomName>?</vdomName>
           <!--Zero or more repetitions:-->
           <!--type: unsignedLong-->
           <vdomID>?</vdomID>
        </addDeviceIDVdom>
     </r20:editAdom>
  </soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.

Request Field	Description
<password>	Administrator password options: • Enter the administrator password • Leave field blank for no password
<name>	The name of the ADOM to be edited.
<version>	Firmware version options: • `400`: FortiOS version 4.0. • `500`: FortiOS version 5.0.
<mr>	The firmware major release version.
<state>	Device ADOM state options: • `true`: ADOMs are enabled • `false`: ADOMs are disabled
<isBackupMode>	Backup Mode ADOM options: • `true`: `BackupMode` is enabled. • `false`: `BackupMode` is disabled.
<VPNManagement>	VPN console ADOM options: • `true`: VPN console is enabled. • `false`: VPN console is disabled.
<metafields>	XML structure consists of metafield data. These strings occur in pairs in XML responses.
<name>	Name of device metafield (s).
<value>	Value of device metafield (s).
<addDeviceSNVdom>	XML structure consists of serial number, VDOM name, and VDOM ID variables.
<SN>	Serial number of device, FGT60C3G06500185, for example.
<vdomName>	The name of the VDOM.
<vdomID>	The VDOM identifier.
<addDeviceIDVdom>	XML structure consists of the device ID, VDOM name, and VDOM ID variables.
<ID>	The ID of the device.
<vdomName>	The name of the VDOM.
<vdomID>	The VDOM identifier.

The response indicates if the request was successful or if it failed.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:editAdom>
      <servicePass>
         <userID>admin</userID>
         <password></password>
      </servicePass>
      <name>NewADOM</name>
      <version>500</version>
      <mr>2</mr>
      <state>true</state>
      <metafields>
         <metafield>
            <name>Used</name>
            <value>true</value>
         </metafield>
      </metafields>
   </r20:editAdom>
</soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:editAdomResponse>
         <errorMsg>
         <errorCode>0</errorCode>
            <errorMsg>Edit adom NewADOM successfully</errorMsg>
         </errorMsg>
   </ns3:editAdomResponse>
</SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • 0: Edited ADOM name successfully. • -101: The ADOM name cannot be empty. The ADOM name is invalid. Version only accepts 400 or 500 values. Invalid major release value. The ADOM metafield does not exist. The metafield name does not exist. Failed to change ADOM information. • -102: The global workspace is locked. Failed to get ADOM information. Failed to get ADOM flags. Failed to create device fetch. Cannot change mode to backup mode since the ADOM has device(s). Cannot get ADOM metafields. • -104: Adding members to ADOM failed.
<errorMsg>	

getAdomList

Use this request to get a list of the ADOMs defined on your FortiManager unit. Only an administrator with the `Super_User` profile can run this command.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getAdomList>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>?</userID>
         <!--Optional:-->
         <!--type: string-->
         <password>?</password>
      </servicePass>
      <!--Optional:-->
      <!--type: string-->
      <detail>?</detail>
   </r20:getAdomList>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: • Enter the administrator password • Leave field blank for no password
<detail>	Detail field options: true or false

The response is a series of <return> tags, each containing information about an ADOM.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getAdomList>
      <servicePass>
         <userID>admin</userID>
         <password></password>
      </servicePass>
      <!--Optional:-->
      <!--type: string-->
      <detail>true</detail>
   </r20:getAdomList>
</soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getAdomListResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>get adom detail list successfully</errorMsg>
      </errorMsg>
      <adomDetail>
         <oid>3</oid>
         <name>root</name>
         <description/>
         <version>500</version>
         <mr>4</mr>
         <state>true</state>
         <isBackupMode>false</isBackupMode>
         <VPNManagement>true</VPNManagement>
      </adomDetail>
      <adomDetail>
         <oid>102</oid>
         <name>others</name>
         <description/>
         <version>500</version>
         <mr>4</mr>
         <state>true</state>
         <isBackupMode>false</isBackupMode>
         <VPNManagement>true</VPNManagement>
      </adomDetail>
      <adomDetail>
         <oid>103</oid>
         <name>FortiCarrier</name>
         <description/>
         <version>500</version>
         <mr>4</mr>
         <state>true</state>
         <isBackupMode>false</isBackupMode>
         <VPNManagement>true</VPNManagement>
      </adomDetail>
      <adomDetail>
         <oid>105</oid>
         <name>FortiMail</name>
         <description/>
         <version>500</version>
         <mr>0</mr>
         <state>true</state>
         <isBackupMode>false</isBackupMode>
         <VPNManagement>true</VPNManagement>
      </adomDetail>
      <adomDetail>
         <oid>107</oid>
         <name>FortiAnalyzer</name>
         <description/>
         <version>500</version>
         <mr>4</mr>
         <state>true</state>
         <isBackupMode>false</isBackupMode>
```

```
      <VPNManagement>true</VPNManagement>
    </adomDetail>
    <adomDetail>
      <oid>109</oid>
      <name>FortiWeb</name>
      <description/>
      <version>500</version>
      <mr>0</mr>
      <state>true</state>
      <isBackupMode>false</isBackupMode>
      <VPNManagement>true</VPNManagement>
    </adomDetail>
    <adomDetail>
      <oid>111</oid>
      <name>FortiCache</name>
      <description/>
      <version>300</version>
      <mr>0</mr>
      <state>true</state>
      <isBackupMode>false</isBackupMode>
      <VPNManagement>true</VPNManagement>
    </adomDetail>
    <adomDetail>
      <oid>113</oid>
      <name>FortiClient</name>
      <description/>
      <version>500</version>
      <mr>0</mr>
      <state>true</state>
      <isBackupMode>false</isBackupMode>
      <VPNManagement>true</VPNManagement>
    </adomDetail>
    <adomDetail>
      <oid>114</oid>
      <name>Syslog</name>
      <description/>
      <version>0</version>
      <mr>0</mr>
      <state>true</state>
      <isBackupMode>false</isBackupMode>
      <VPNManagement>true</VPNManagement>
    </adomDetail>
    <adomDetail>
      <oid>116</oid>
      <name>FortiManager</name>
      <description/>
      <version>500</version>
      <mr>4</mr>
      <state>true</state>
      <isBackupMode>false</isBackupMode>
      <VPNManagement>false</VPNManagement>
    </adomDetail>
    <adomDetail>
      <oid>118</oid>
      <name>FortiSandbox</name>
      <description/>
      <version>200</version>
```

```
            <mr>1</mr>
            <state>true</state>
            <isBackupMode>false</isBackupMode>
            <VPNManagement>true</VPNManagement>
         </adomDetail>
         <adomDetail>
            <oid>120</oid>
            <name>FortiDDoS</name>
            <description/>
            <version>400</version>
            <mr>1</mr>
            <state>true</state>
            <isBackupMode>false</isBackupMode>
            <VPNManagement>true</VPNManagement>
         </adomDetail>
         <adomDetail>
            <oid>133</oid>
            <name>NewADOM</name>
            <description/>
            <version>500</version>
            <mr>2</mr>
            <state>true</state>
            <isBackupMode>false</isBackupMode>
            <VPNManagement>false</VPNManagement>
         </adomDetail>
      </ns3:getAdomListResponse>
   </SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • 0: Retrieved ADOM list successfully. Retrieved ADOM detail list successfully. • -104: ADOM fetch error. Cannot get ADOM basic information. Cannot get ADOM detail information. • -106: Not enough memory.
<errorMsg>	
<adomDetail>	XML structure consists of the object identifier, ADOM name, and description.
<oid>	The object identifier.
<name>	The ADOM name.
<description>	A description of the ADOM.
<version>	Firmware version options: • `400`: FortiOS version 4.0. • `500`: FortiOS version 5.0.

Response Field	Description
<mr>	The firmware major release version.
<state>	Device ADOM state options: • `true`: ADOMs are enabled. • `false`: ADOMs are disabled.
<isBackupMode>	Backup Mode ADOM options: • `true`: `BackupMode` is enabled. • `false`: `BackupMode` is disabled.
<VPNManagement>	VPN console ADOM options: • `true`: VPN console is enabled. • `false`: VPN console is disabled.
<metafield>	XML structure consists of metafield data. These strings occur in pairs in XML responses.
<name>	Name of device metafield (s).
<value>	Value of device metafield (s).

getAdoms

Use this request to get a list of ADOMs.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getAdoms>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>?</userID>
         <!--Optional:-->
         <!--type: string-->
         <password>?</password>
      </servicePass>
      <!--Zero or more repetitions:-->
      <!--type: string-->
      <names>?</names>
      <!--Zero or more repetitions:-->
      <!--type: string-->
      <adomIds>?</adomIds>
   </r20:getAdoms>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: • Enter the administrator password. • Leave field blank for no password.
<names>	The ADOM name.
<adomIDs>	The ADOM object ID.

The response indicates if the request was successful or if it failed.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getAdoms>
      <servicePass>
         <userID>admin</userID>
         <password></password>
      </servicePass>
      <names>root</names>
      <adomIds>3</adomIds>
   </r20:getAdoms>
</soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getAdomsResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>Get adoms info Successfully</errorMsg>
      </errorMsg>
      <adomDetail>
         <oid>3</oid>
         <name>root</name>
         <description/>
         <version>500</version>
         <mr>4</mr>
         <state>true</state>
         <isBackupMode>false</isBackupMode>
         <VPNManagement>false</VPNManagement>
         <metafields>
            <metafield>
               <name>Metfield1</name>
               <value>True</value>
            </metafield>
         </metafields>
      </adomDetail>
```

```
    </ns3:getAdomsResponse>
  </SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • 0: Retrieved ADOM information successfully. • -101: Invalid admin user name. User does not have permission to run this command. Cannot get ADOM OID. • -102: Cannot get ADOM detail information. • -104: Cannot get ADOM detail information. • -106: Not enough memory.
<errorMsg>	
<adomDetail>	XML structure consists of the object identifier, ADOM name, description, firmware version, and major release.
<oid>	The object identifier for the ADOM.
<name>	The name of the ADOM.
<description>	A description of the ADOM.
<version>	Firmware version options: • `400`: FortiOS version 4.0. • `500`: FortiOS version 5.0.
<mr>	The firmware major release version.
<state>	Device ADOM state options: • `true`: ADOMs are enabled. • `false`: ADOMs are disabled.
<isBackupMode>	Backup Mode ADOM options: • `true`: `BackupMode` is enabled. • `false`: `BackupMode` is disabled.
<VPNManagement>	VPN console ADOM options: • `true`: VPN console is enabled. • `false`: VPN console is disabled.
<metafield>	XML structure consists of metafield data. These strings occur in pairs in XML responses.
<name>	Name of device metafield (s).
<value>	Value of device metafield (s).

getDeviceList

Use this request to get summary information about the managed devices, optionally limited to a particular ADOM.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getDeviceList>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>?</userID>
         <!--Optional:-->
         <!--type: string-->
         <password>?</password>
      </servicePass>
      <!--Optional:-->
      <!--type: string-->
      <adom>?</adom>
      <!--Optional:-->
      <!--type: string-->
      <detail>?</detail>
   </r20:getDeviceList>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: • Enter the administrator password. • Leave field blank for no password.
<adom>	If the ADOM field is blank, the default ADOM will be that of the administrative user. If this administrator binds to all ADOMs, then the ADOM is root.
<detail>	Detail field options: true, or false

The response is a series of <return> tags, each containing information about a device.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getDeviceList>
      <servicePass>
         <userID>admin</userID>
```

```
            <password></password>
         </servicePass>
         <adom>NewADOM</adom>
         <detail>true</detail>
      </r20:getDeviceList>
   </soapenv:Body>
```

Example response: (detail is false)

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getDeviceListResponse>
         <errorMsg>
            <errorCode>0</errorCode>
            <errorMsg>get device detail list successfully</errorMsg>
         </errorMsg>
         <deviceDetail>
            <devId>129</devId>
            <firmware>FortiGate</firmware>
            <firmwareVersion>500</firmwareVersion>
            <buildNum>128</buildNum>
            <description/>
            <hostname>FGT60C3000000000</hostname>
            <platform>FortiGate-60C</platform>
            <sn>FGT60C3000000000</sn>
            <ip>1.2.6.7</ip>
            <IPSContract/>
            <antiVirusContract>19.00(2019-10-19 08:31)</antiVirusContract>
            <appsignature/>
            <mgmtMode>reg</mgmtMode>
         </deviceDetail>
   </ns3:getDeviceListResponse>
</SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • 0: Retrieved device list successfully. Retrieved device detail list successfully. • -102: Device fetch error for ADOM. • -104: Cannot get device detail information.
<errorMsg>	
<deviceDetail>	XML structure consists of the following tags.
<devID>	The Device ID. This is the primary device identifier.
<firmware>	FortiGate, FortiCarrier, or FortiSwitch
<firmwareVersion>	Version of device operating system, 5, for example for FortiOS 5.0.

Response Field	Description
<buildNum>	Firmware version build number, 0128, for example.
<description>	Device description from FortiManager database.
<hostname>	The device host name.
<platform>	Platform name for device, FortiGate-60C, for example.
<sn>	Serial number of device.
<ip>	IP address of device network interface from which response was received.
<IPSContract>	FortiGuard IPS definitions version and last update time, 2.00461(2008-12-08 11:23), for example.
<antiVirusContract>	AV contract and expiry date, 8.00631(2012-02-15 14:27), for example.
<appsignature>	FortiGuard application signature.
<mgmtMode>	The device management mode. One of the following: • `reg`: Registered device • `unreg`: Unregistered device • `unknown`: Device registration status is unknown.

getDevices

Use this request to get information about specific managed devices, identified by serial number or device ID. You can obtain device ID values by using the `execute dmserver showdev` CLI command.

If you want information about the device's configuration, see getFazConfig on page 38.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getDevices>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>?</userID>
         <!--Optional:-->
         <!--type: string-->
         <password>?</password>
      </servicePass>
      <!--Zero or more repetitions:-->
      <!--type: string-->
      <serialNumbers>?</serialNumbers>
      <!--Zero or more repetitions:-->
```

```
      <!--type: unsignedLong-->
      <devIds>?</devIds>
   </r20:getDevices>
</soapenv:Body>
```

Request Field		Description
<servicePass>		XML structure consists of username and password variables.
	<userID>	The administrator user name.
	<password>	Administrator password options: • Enter the administrator password. • Leave field blank for no password.
<serialNumbers>		Serial number of the device. This is the secondary identifier. You can enter multiple serial numbers fields.
<devIds>		Device ID. This is the primary device identifier. You can omit this field and use the serial number instead. You can enter multiple device ID fields.

The response is a series of <return> tags, each containing information about a device.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getDevices>
         <servicePass>
            <password></password>
            <userID>admin</userID>
         </servicePass>
         <serialNumbers>FGT60C0000000000</serialNumbers>
         <serialNumbers>FGT60C0000000001</serialNumbers>
   </r20:getDevices>
</soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getDevicesResponse>
         <return>
            <firmware>FortiGate</firmware>
            <firmwareVersion>5</firmwareVersion>
            <buildNum>128</buildNum>
            <description/>
            <hostname>Dev3</hostname>
            <IPSContract>8.442(2018-09-31 11:23)</IPSContract>
            <antiVirusContract>15.378(2017-11-15 13:59)</antiVirusContract>
            <platform>FortiGate-60C</platform>
            <sn>FGT60C0000000000</sn>
            <ip>1.2.1.16</ip>
         </return>
```

```
            <return>
               <firmware>FortiGate</firmware>
               <firmwareVersion>5</firmwareVersion>
               <buildNum>128</buildNum>
               <description/>
               <hostname>FGT60C0000000001</hostname>
               <IPSContract/>
               <antiVirusContract/>
               <platform>Fortigate-60C</platform>
               <sn>FGT60C0000000001</sn>
               <ip>1.2.1.12</ip>
            </return>
      </ns3:getDevicesResponse>
   </SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • 0: Retrieved device(s) information successfully. • -102: Serial number is not found. Cannot get device information. • -104: Cannot get device information.
<errorMsg>	
<firmware>	One of: • FortiGate • FortiCarrier • FortiSwitch
<firmwareVersion>	Version of device operating system, 500, for example for FortiOS 5.0.
<buildNum>	Firmware version build number, 0128, for example.
<description>	Device description from database.
<hostname>	The device host name.
<IPSContract>	FortiGuard IPS definitions version and last update time, 2.00461(2012-11-08 11:23), for example.
<antiVirusContract>	AV contract and expiry date, 8.00631(2012-02-15 14:27), for example.
<platform>	Platform name for device, FortiGate-60C, for example.
<sn>	Serial number of device, FGT60C3G06500185, for example.
<ip>	IP address of device network interface from which response was received.

getDeviceVdomList

Use this request to obtain a list of device VDOMs.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getDeviceVdomList>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>?</userID>
         <!--Optional:-->
         <!--type: string-->
         <password>?</password>
      </servicePass>
      <!--Optional:-->
      <!--type: string-->
      <devName>?</devName>
      <!--Optional:-->
      <!--type: unsignedLong-->
      <devID>?</devID>
   </r20:getDeviceVdomList>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<devName>	Name of the device host.
<devId>	The Device ID. This is the primary device identifier.

The response indicates if the request was successful or if it failed.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getDeviceVdomList>
      <servicePass>
         <userID>admin</userID>
         <password></password>
      </servicePass>
      <devName>500D</devName>
```

```
      <devID>500D</devID>
   </r20:getDeviceVdomList>
</soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getDeviceVdomListResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>Get device 412 vdom list successfully</errorMsg>
      </errorMsg>
      <name>500D</name>
      <oid>412</oid>
      <return>
         <name>root</name>
         <oid>3</oid>
      </return>
      <return>
         <name>vdom1</name>
         <oid>101</oid>
      </return>
   </ns3:getDeviceVdomListResponse>
</SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • 0: Retrieved device VDOM list successfully. • -101: Cannot find the device by provided name or ID.
<errorMsg>	
<name>	The name of the VDOM device list.
<oid>	The object identifier.

getFazArchive

Use this request to get a FortiAnalyzer archive file. You need to input the device ID, archive type, and the archive file name.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getFazArchive>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
```

```
            <userID>admin</userID>
            <!--Optional:-->
            <!--type: string-->
            <password></password>
         </servicePass>
         <!--Optional:-->
         <!--type: string-->
         <adom>root</adom>
         <!--Optional:-->
         <!--type: string-->
         <devId>?</devId>
         <!--Optional:-->
         <!--type: string-->
         <vdom>?</vdom>
         <!--Optional:-->
         <!--type: archiveTypes - enumeration: [web,email,ftp,IM,MMS,quarantine,IPS]-->
         <type>?</type>
         <!--Optional:-->
         <!--type: string-->
         <fileName>?</fileName>
         <!--Optional:-->
         <!--type: string-->
         <checksum>?</checksum>
         <!--Optional:-->
         <!--type: string-->
         <zipPassword>?</zipPassword>
         <!--Optional:-->
         <!--type: compressionType - enumeration: [tar,gzip]-->
         <compression>tar</compression>
      </r20:getFazArchive>
   </soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<adom>	The ADOMs for which you want to get archives from.
<devId>	The device ID you want to get archives from.
<vdom>	The VDOM you want to get archives from.
<type>	The archive type. Archive type options: *Web*, *Email*, *FTP*, *IM*, *MMS*, *Quarantine*, or *IPS*.
<fileName>	The archive file name. You can check the name under *Log View* > *Archive*.
<checksum>	The checksum value.

Request Field	Description
<zipPassword>	The password set for the zip file.
<compression>	The compression method.
<filelist>	The archive file list.
<filename>	The archive file name will be displayed under this element.
<data>	The archive file content data. The data is base64 encoded, you need to decode the data before use.

The response will contain the binary data if the archive file in a base64 encoded message.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getFazArchive>
      <servicePass>
         <userID>admin</userID>
         <password></password>
      </servicePass>
      <adom>root</adom>
      <devId>FG200B0000000001</devId>
      <type>IPS</type>
      <fileName>50005:0</fileName>
      <zipPassword></zipPassword>>
   </r20:getFazArchive>
</soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getFazArchiveResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>getFazArchive successfully</errorMsg>
      </errorMsg>
      <fileList>
      <fileName>50005:0</fileName>
         <data>
         =</data>
         <error>None</error>
      </fileList>
   </ns3:getFazArchiveResponse>
</SOAP-ENV:Body>
```

Request Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • -101: Invalid username, password, or ADOM. Cannot get device ID. Cannot get file name. Cannot get type. Cannot get checksum. Cannot get content filename. • -104: Cannot get content archive. Get FortiAnalyzer archive failed, no such file name. Get FortiAnalyzer archive failed, error reading file name. • -106: Not enough memory.
<errorMsg>	
<filelist>	The archive file list.
<filename>	The archive file name will be displayed under this element.
<data>	The archive file content data. The data is base64 encoded, you need to decode the data before use.

getFazConfig

Use this request to get the FortiAnalyzer configuration.

Request options:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getFazConfig>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>?</userID>
         <!--Optional:-->
         <!--type: string-->
         <password>?</password>
      </servicePass>
   </r20:getFazConfig>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.

The response indicates if the request was successful or if it failed.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getFazConfig>
      <servicePass>
         <userID>admin</userID>
         <password></password>
      </servicePass>
   </r20:getFazConfig>
</soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getFazConfigResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>getFazConfig successfully</errorMsg>
      </errorMsg>
      <config>#config-version=FAZVM64-5.4-FW-build0949-151002
         config system global
            set adom-mode normal
            set adom-status enable
            set hostname "FAZVM64"
         end
         config system interface
            edit "port1"
               set ip 172.172.172.222 255.255.255.0
               set allowaccess ping https ssh snmp telnet http webservice aggregator fgfm
               config ipv6
            end
            next
            edit "port2"
               set allowaccess https http webservice
               config ipv6
            end
            next
         end
         config system snmp sysinfo
         end
         config system route
            edit 1
               set device "port1"
               set gateway 172.172.172.1
            next
         end
         config system dns
            set primary 208.91.112.53
            set secondary 208.91.112.63
         end
         config system ntp
            config ntpserver
               edit 1
```

```
            set server "ntp1.fortinet.net"
         next
      end
      set status enable
   end
   config system certificate oftp
   end
   config system backup all-settings
   end
   config system admin profile
      edit "Restricted_User"
         set description "Restricted user profiles have no System Privileges enabled,
             and have read-only access for all Device Privileges."
         set device-manager read
         set realtime-monitor read
         set log-viewer read
         set report-viewer read
         set event-management read
      next
      edit "Standard_User"
         set description "Standard user profiles have no System Privileges enabled,
             but have read/write access for all Device Privileges."
         set adom-switch read-write
         set device-manager read-write
         set device-op read-write
         set realtime-monitor read-write
         set log-viewer read-write
         set report-viewer read-write
         set event-management read-write
      next
      edit "Super_User"
         set description "Super user profiles have all system and device privileges
             enabled."
         set system-setting read-write
         set adom-switch read-write
         set device-manager read-write
         set device-op read-write
         set realtime-monitor read-write
         set log-viewer read-write
         set report-viewer read-write
         set event-management read-write
      next
   end
   config system certificate ca
   end
   config system certificate local
   end
   config system password-policy
   end
   config system admin user
      edit "admin"
         set profileid "Super_User"
         set adom "all_adoms"
         set policy-package "all_policy_packages"
         set rpc-permit read-write
         config dashboard
            edit 1
```

```
      set name "System Information"
      set column 1
      set refresh-interval 0
      set tabid 1
      set widget-type sysinfo
   next
   edit 2
      set name "System Resources"
      set column 1
      set refresh-interval 0
      set tabid 1
      set widget-type sysres
      set res-view-type real-time
      set res-cpu-display each
   next
   edit 3
      set name "License Information"
      set column 2
      set refresh-interval 0
      set tabid 1
      set widget-type licinfo
   next
   edit 4
      set name "Unit Operation"
      set column 2
      set refresh-interval 0
      set tabid 1
      set widget-type sysop
   next
   edit 5
      set name "Log Receive Monitor"
      set column 1
      set refresh-interval 0
      set tabid 1
      set widget-type top-lograte
      set log-rate-topn 1
   next
   edit 6
      set name "Logs/Data Received"
      set column 2
      set refresh-interval 0
      set tabid 1
      set widget-type logrecv
      set res-view-type real-time
      set res-cpu-display each
   next
   edit 7
      set name "Statistics"
      set column 2
      set refresh-interval 0
      set tabid 1
      set widget-type statistics
   next
   edit 8
      set name "Insert Rate vs Receive Rate"
      set column 2
      set refresh-interval 0
```

```
            set tabid 1
            set widget-type logdb-perf
         next
         edit 9
            set name "Log Insert Lag Time"
            set column 2
            set refresh-interval 0
            set tabid 1
            set widget-type logdb-lag
         next
         edit 10
            set name "Disk I/O"
            set column 1
            set refresh-interval 0
            set tabid 1
            set widget-type disk-io
         next
         edit 11
            set name "Alert Message Console"
            set column 2
            set refresh-interval 0
            set tabid 1
            set widget-type alert
            set num-entries 0
         next
         edit 12
            set name "CLI Console"
            set column 1
            set refresh-interval 0
            set tabid 1
            set widget-type jsconsole
         next
      end
   next
end
config system admin setting
end
config system alertemail
end
config system alert-console
end
config system locallog disk setting
end
config system locallog disk filter
end
config system locallog memory setting
end
config system locallog memory filter
end
config system locallog fortianalyzer filter
end
config system locallog fortianalyzer2 filter
end
config system locallog fortianalyzer3 filter
end
config system locallog fortianalyzer setting
end
```

```
config system locallog fortianalyzer2 setting
end
config system locallog fortianalyzer3 setting
end
config system locallog syslogd setting
end
config system locallog syslogd filter
end
config system locallog syslogd2 setting
end
config system locallog syslogd2 filter
end
config system locallog syslogd3 setting
end
config system locallog syslogd3 filter
end
config system locallog setting
end
config system fips
end
config system central-management
end
config fmupdate av-ips fgt server-override
end
config fmupdate av-ips fct server-override
end
config fmupdate av-ips push-override
end
config fmupdate av-ips push-override-to-client
end
config fmupdate av-ips web-proxy
end
config fmupdate fct-services
end
config fmupdate av-ips advanced-log
end
config fmupdate av-ips update-schedule
end
config fmupdate analyzer virusreport
end
config fmupdate service
end
config fmupdate publicnetwork
end
config fmupdate disk-quota
end
config fmupdate server-access-priorities
end
config fmupdate device-version
end
config fmupdate server-override-status
end
config fmupdate multilayer
end
config fmupdate support-pre-fgt43
end
config fmupdate fds-setting
```

```
end
config system log alert
end
config system log settings
   config rolling-regular
   end
end
config system aggregation-service
end
config system sql
   config ts-index-field
      edit "FGT-app-ctrl"
         set value "user,group,srcip,dstip,dstport,service,app,action,hostname"
      next
      edit "FGT-attack"
         set value "severity,srcip,dstip,action,user,attack"
      next
      edit "FGT-content"
         set value "from,to,subject,action,srcip,dstip,hostname,status"
      next
      edit "FGT-dlp"
         set value "user,srcip,service,action,filename"
      next
      edit "FGT-emailfilter"
         set value "user,srcip,from,to,subject"
      next
      edit "FGT-event"
         set value "subtype,ui,action,msg"
      next
      edit "FGT-traffic"
         set value "user,srcip,dstip,service,app,utmaction"
      next
      edit "FGT-virus"
         set value "service,srcip,dstip,action,filename,virus,user"
      next
      edit "FGT-voip"
         set value "action,user,src,dst,from,to"
      next
      edit "FGT-webfilter"
         set value "user,srcip,dstip,service,action,catdesc,hostname"
      next
      edit "FGT-netscan"
         set value "user,dstip,vuln,severity,os"
      next
      edit "FGT-fct-event"
      next
      edit "FGT-fct-traffic"
      next
      edit "FGT-fct-netscan"
      next
      edit "FML-emailfilter"
         set value "client_name,dst_ip,from,to,subject"
      next
      edit "FML-event"
         set value "subtype,msg"
      next
      edit "FML-history"
```

```
                set value "classifier,disposition,from,to,client_
                    name,direction,domain,virus"
              next
              edit "FML-virus"
                set value "src,msg,from,to"
              next
              edit "FWB-attack"
                set value "http_host,http_url,src,dst,msg,action"
              next
              edit "FWB-event"
                set value "ui,action,msg"
              next
              edit "FWB-traffic"
                set value "src,dst,service,http_method,msg"
              next
              end
            set start-time 00:00 2000/01/01
          end
          config system report est-browse-time
          end
          config system report auto-cache
          end
          config system report setting
          end
          config system fortiview setting
          end
          config system auto-delete
          config dlp-files-auto-deletion
          end
          config log-auto-deletion
          end
          config quarantine-files-auto-deletion
          end
          config report-auto-deletion
          end
        end</config>
      </ns3:getFazConfigResponse>
    </SOAP-ENV:Body>
```

Request Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • -101: Invalid username or password. • -102: Cannot allocate temp file. Cannot create configuration file. Cannot open file. • -106: Not enough memory.
<errorMsg>	
<config>	The device configuration.

getFazGeneratedReports

Use this request to get a completed historical report. To use this command, you need to input the report name, report date, and compression method in the request.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getFazGeneratedReport>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>?</userID>
         <!--Optional:-->
         <!--type: string-->
         <password>?</password>
      </servicePass>
      <!--Optional:-->
      <!--type: string-->
      <adom>?</adom>
      <!--Optional:-->
      <!--type: string-->
      <reportDate>?</reportDate>
      <!--Optional:-->
      <!--type: string-->
      <reportName>?</reportName>
      <!--Optional:-->
      <!--type: compressionType - enumeration: [tar,gzip]-->
      <compression>tar</compression>
   </r20:getFazGeneratedReport>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<adom>	The ADOMs for which you want to get a report from.
<reportDate>	The report generation date; in the format YYYY_MM_DD.
<reportName>	The generated report name. For example, S-4_t4-VPN Report-2015-10-07-0820. The listFazGeneratedReports command can be used to determine the names of the reports.
<compression>	The compression type of the report that will be returned by this command. Compression options include: `tar`, and `gzip`.

The report data returned in the response message is base64 encoded binary data. You need to decode it and then decompress it to get the report files.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getFazGeneratedReport>
      <servicePass>
         <userID>admin</userID>
         <password></password>
      </servicePass>
      <adom>root</adom>
      <reportDate>2015_10_07</reportDate>
      <reportName>S-4_t4-VPN Report-2015-10-07-0820</reportName>
      <compression>tar</compression>
   </r20:getFazGeneratedReport>
</soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getFazGeneratedReportResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>getFazGeneratedReport successfully</errorMsg>
      </errorMsg>
      <reportName>S-4_t4-VPN Report-2015-10-07-0820</reportName>
      <size>460800</size>
      <fazReportData>
         <reportContent>Uy00X3Q0LVZQTiBSZXBvcnQtMjAxNS0xMC0wNy0wODIwLwAAAAAAAAAA...
      </fazReportData>
   </ns3:getFazGeneratedReportResponse>
</SOAP-ENV:Body>
```

Request Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • -101: Invalid username, password, or ADOM. Cannot get report name. Cannot get report date. • -104: Cannot find report name. Cannot find file in directory. Cannot read file in directory. • -106: Not enough memory.
<errorMsg>	
<reportName>	The generated report name. For example, S-schedule-utm-reports_t1-2013-01-24-1022.
<size>	The generated report size.

Request Field	Description
<fazReportData>	Report content data will be displayed under this element.
<reportContent>	Contains the actual report data. The data is base64 encoded, you need to decode the data before use.

getSystemStatus

Use this request to get system status information in the current system.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getSystemStatus>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>?</userID>
         <!--Optional:-->
         <!--type: string-->
         <password>?</password>
      </servicePass>
      <!--Optional:-->
      <!--type: string-->
      <adom>?</adom>
   </r20:getSystemStatus>
</soapenv:Body>
```

Request Field		Description
<servicePass>		XML structure consists of username and password variables.
	<userID>	The administrator user name.
	<password>	Administrator password options: • Enter the administrator password. • Leave field blank for no password.
<adom>		If the ADOM field is blank, it is assigned as root.

The response indicates if the request was successful or if it failed.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getSystemStatus>
      <servicePass>
         <userID>admin</userID>
```

```
            <password></password>
      </servicePass>
      <adom>root</adom>
      </r20:getSystemStatus>
   </soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getSystemStatusResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>getSystemStatus successfully</errorMsg>
      </errorMsg>
      <platformType>FAZVM64</platformType>
      <version>v5.4.0-build0952</version>
      <serialNumber>FAZ-VM0000000001</serialNumber>
      <biosVersion>04000012</biosVersion>
      <hostName>FAZVM64</hostName>
      <maxNumAdminDomains>10000</maxNumAdminDomains>
      <maxNumDeviceGroup>10000</maxNumDeviceGroup>
      <adminDomainConf>Enabled</adminDomainConf>
      <fipsMode>Disabled</fipsMode>
      <diskSpaceFreeMB>78141</diskSpaceFreeMB>
      <diskSpaceUsedMB>2481</diskSpaceUsedMB>
   </ns3:getSystemStatusResponse>
</SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • -101: Invalid username, password, or ADOM.
<errorMsg>	
<platformType>	Device model information.
<version>	The firmware version.
<serialNumber>	The serial number of the device.
<biosVersion>	The BIOS version of the device.
<hostName>	The device host name.
<maxNumAdminDomains>	The maximum number of ADOMs.
<maxNumDeviceGroup>	The maximum number of device groups.
<adminDomainConf>	ADOM mode status.

Response Field	Description
<fipsMode>	FIPS mode status.
<diskSpaceFreeMB>	The amount of disk space that is available, in MB.
<diskSpaceUsedMB>	The amount of disk space that is used, in MB.

getTaskList

Use this request to get a list of tasks as defined on your unit. Only an administrator with the `Super_User` profile can run this command.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getTaskList>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>?</userID>
         <!--Optional:-->
         <!--type: string-->
         <password>?</password>
      </servicePass>
      <!--Optional:-->
      <!--type: string-->
      <adom>?</adom>
      <!--type: string-->
      <taskId>?</taskId>
   </r20:getTaskList>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: • Enter the administrator password. • Leave field blank for no password.
<adom>	If the ADOM field is blank, the default ADOM will be that of the administrative user. If this administrator binds to all ADOMs, then the ADOM is root.
<taskId>	Indicates the task ID number. If the `<waitTask>` was false, then the task ID is displayed.

The response is a series of <return> tags, each containing information about a task.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getTaskList>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>admin</userID>
         <!--Optional:-->
         <!--type: string-->
         <password></password>
      </servicePass>
      <!--Optional:-->
      <!--type: string-->
      <adom></adom>
      <!--type: string-->
      <taskId>2</taskId>
   </r20:getTaskList>
</soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getTaskListResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>Get task ID detail successfully</errorMsg>
      </errorMsg>
      <taskList>
         <taskId>2</taskId>
         <source>0</source>
         <description>adddevtitle</description>
         <userID>admin</userID>
         <status>5</status>
         <startTime>2015-10-06T12:55:34Z</startTime>
         <deviceList>
            <devName>FMG-VM64</devName>
            <ip>1.1.1.2</ip>
            <status>5</status>
            <message>restrictedprod</message>
            <history>
               <name>FMG-VM64</name>
               <percentage>100</percentage>
               <description>2015-10-06 05:55:34:restrictedprod</description>
            </history>
         </deviceList>
      </taskList>
   </ns3:getTaskListResponse>
</SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • 0: Retrieved task ID detail successfully. • -101: Invalid task ID. The task ID is empty or invalid. • -102: The task ID does not exist. • -106: Not enough memory.
<errorMsg>	
<taskList>	XML structure consists of the task ID, source, description, user ID, status, and start time variables.
<taskId>	Indicates the task ID number. If the `<waitTask>` was false, then the task ID is displayed.
<source>	Indicates the source of the task: • 0: Device manager • 1: Security console • 2: Copy global object • 3: Install configuration • 4: Script execution • 5: System checkpoint • 6: Import device policy • 7: Install EMS global policy
<description>	Describes the list.
<userID>	The administrator user name.
<status>	Indicates the status of the task: • 1: running • 2: cancelling • 3: cancelled • 4: done • 5: error • 6: aborting • 7: aborted
<startTime>	Indicates the time the task list started.
<deviceList>	XML structure consists of the device name, IP, status, message, and history.
<devName>	Name of the device host.

Response Field	Description
<ip>	The device IP address.
<status>	Status of the device.
<message>	Description of the task.
<history>	
<name>	The history name.
<percentage>	Percentage of progress bar of each task that has been applied to the device.
<description>	Description of the history.

listFazGeneratedReports

Use this request to list FortiAnalyzer generated reports.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:listFazGeneratedReports>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>?</userID>
         <!--Optional:-->
         <!--type: string-->
         <password>?</password>
      </servicePass>
      <!--Optional:-->
      <!--type: string-->
      <adom>?</adom>
      <!--Optional:-->
      <!--type: dateTime-->
      <startDate>?</startDate>
      <!--Optional:-->
      <!--type: dateTime-->
      <endDate>?</endDate>
   </r20:listFazGeneratedReports>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.

Request Field	Description
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<adom>	The ADOMs for which you want to list a generated reports.
<startDate>	The report start date, for example: 1999-12-31T23:59:59.
<endDate>	The report end date.

The response indicates if the request was successful or if it failed.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:listFazGeneratedReports>
      <servicePass>
         <userID>admin</userID>
         <password></password>
      </servicePass>
      <adom>root</adom>
      <startDate>1970-01-01T00:00:00</startDate>
      <endDate>2015-10-10T00:00:00</endDate>
   </r20:listFazGeneratedReports>
</soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:listFazGeneratedReportsResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>listFazGeneratedReports successfully</errorMsg>
      </errorMsg>
      <totalNumberExists>2</totalNumberExists>
      <reportList>
         <reportName>S-10023_t10023-PCI-DSS Compliance Review-2015-10-07-0820</reportName>
         <startTime>2015-10-07T15:20:12Z</startTime>
         <endTime>2015-10-07T15:20:14Z</endTime>
         <reportProgressPercent>100</reportProgressPercent>
         <size>0</size>
         <formats>PHX</formats>
      </reportList>
      <reportList>
         <reportName>S-4_t4-VPN Report-2015-10-07-0820</reportName>
         <startTime>2015-10-07T15:20:18Z</startTime>
         <endTime>2015-10-07T15:20:20Z</endTime>
         <reportProgressPercent>100</reportProgressPercent>
         <size>0</size>
         <formats>PHX</formats>
```

```
      </reportList>
   </ns3:listFazGeneratedReportsResponse>
</SOAP-ENV:Body>
```

Request Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • -101: Invalid username, password, or ADOM. No reports are available. • -104: Cannot get report counts. • -106: Not enough memory.
<errorMsg>	
<totalNumberExists>	The total number of available reports on the FortiAnalyzer.
<reportList>	XML structure consists of report name, start time, end time, report progress, size, and format variables.
<reportName>	The generated report name. For example S-8_t8-DocReport-2015-10-07-0845.
<startTime>	Indicates the time the report started.
<endTime>	Indicates the time the report ended.
<reportProgressPercent>	Report running progress; 0 to 100%.
<size>	The generated report size.
<formats>	The report format: • P: PDF • H: HTML • T: TXT

removeFazArchive

Use this command to remove a FortiAnalyzer archive.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:removeFazArchive>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>?</userID>
         <!--Optional:-->
```

```
            <!--type: string-->
            <password>?</password>
         </servicePass>
         <!--Optional:-->
         <!--type: string-->
         <adom>?</adom>
         <!--Optional:-->
         <!--type: string-->
         <devId>?</devId>
         <!--Optional:-->
         <!--type: string-->
         <vdom>?</vdom>
         <!--Optional:-->
         <!--type: archiveTypes - enumeration: [web,email,ftp,IM,MMS,quarantine,IPS]-->
         <type>?</type>
         <!--Optional:-->
         <!--type: string-->
         <fileName>?</fileName>
         <!--Optional:-->
         <!--type: string-->
         <checksum>?</checksum>
      </r20:removeFazArchive>
   </soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<adom>	The ADOM for which you want to remove the FortiAnalyzer archive.
<devId>	The device ID. This is the primary device identifier.
<vdom>	The VDOM you want to remove archives from.
<type>	The archive type: `Web`, `Email`, `FTP`, `IM`, `MMS`, `Quarantine`, or `IPS`.
<fileName>	Shows the name of the file. Note: the file name cannot start with a | or a ~ character.
<checksum>	Checksum is used when the type is Quarantine. Checksum is used instead of filename.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getFazArchive>
      <servicePass>
         <userID>admin</userID>
         <password></password>
```

```
      </servicePass>
      <adom>root</adom>
      <devId>FMGVM00000000001</devId>
      <type>IPS</type>
      <fileName>50008:0</fileName>
      <checksum></checksum>
      <zipPassword></zipPassword>
      <compression>tar</compression>
   </r20:getFazArchive>
</soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:removeFazArchiveResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>removeFazArchive successfully</errorMsg>
      </errorMsg>
   </ns3:removeFazArchiveResponse>
</SOAP-ENV:Body>
```

Request Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • -101: Invalid username, password, or ADOM. Cannot get the device ID. Cannot get the file name. Cannot get the type. Cannot get the checksum. • -104: Cannot delete content archive file.
<errorMsg>	

runFazReport

Use this request to run a report through web service. You need to input the schedule name of the report. `runFazReport` supports up to 10k filters.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:runFazReport>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>?</userID>
         <!--Optional:-->
         <!--type: string-->
         <password>?</password>
      </servicePass>
```

```
        <!--Optional:-->
        <!--type: string-->
        <adom>?</adom>
        <!--Optional:-->
        <!--type: string-->
        <reportTemplate>?</reportTemplate>
        <!--Zero or more repetitions:-->
        <!--type: string-->
        <filter>?</filter>
     </r20:runFazReport>
  </soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<adom>	The ADOMs for which you want to run a report against.
<reportTemplate>	The name of the report template.
<filter>	Add filters to create per-user reports.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:runFazReport>
      <servicePass>
         <userID>admin</userID>
         <password></password>
      </servicePass>
      <adom>root</adom>
      <reportTemplate>Away Team Report</reportTemplate>
      <filter>user=Fry</filter>
      <filter>user=Leela</filter>
      <filter>user=Bender</filter>
   </r20:runFazReport>
</soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:runFazReportResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>runFazReport successfully</errorMsg>
      </errorMsg>
      <reportTemplate>Away Team Report</reportTemplate>
   </ns3:runFazReportResponse>
</SOAP-ENV:Body>
```

Request Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • -101: Invalid username, password, or ADOM. Cannot get report schedule name. • -104: Cannot get report schedule name from SQL.
<errorMsg>	
<reportTemplate>	The name of the report template.

searchFazLog

Use this request to provide raw logs in FortiAnalyzer per conditions set in the request. You need to input the log format, device name, log type, search criteria, start index, and maximum return value in the request message body.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:searchFazLog>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>?</userID>
         <!--Optional:-->
         <!--type: string-->
         <password>?</password>
      </servicePass>
      <!--Optional:-->
      <!--type: string-->
      <adom>?</adom>
      <!--Optional:-->
      <!--type: searchContent - enumeration: [logs,contentLogs,localLogs]-->
      <content>logs</content>
      <!--Optional:-->
      <!--type: logFormats - enumeration: [rawFormat,CSV]-->
      <format>rawFormat</format>
      <!--Optional:-->
      <!--type: string-->
      <deviceName>?</deviceName>
      <!--type: logTypes - enumeration:
          [event,traffic,attack,antiVirus,webLogs,IM,email,content,history,generic,voIP,DL
          P,appCtrl,netScan]-->
      <logType>traffic</logType>
      <!--Optional:-->
      <!--type: string-->
      <searchCriteria>?</searchCriteria>
      <!--type: int-->
```

```
        <maxNumMatches>30</maxNumMatches>
        <!--type: int-->
        <startIndex>1</startIndex>
        <!--type: int-->
        <checkArchive>0</checkArchive>
        <!--Optional:-->
        <!--type: archiveTypes - enumeration: [web,email,ftp,IM,MMS,quarantine,IPS]-->
        <DLPArchiveType>?</DLPArchiveType>
        <!--Optional:-->
        <!--type: compressionType - enumeration: [tar,gzip]-->
        <compression>tar</compression>
    </r20:searchFazLog>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<adom>	The ADOMs for which you want to search logs.
<content>	The log contents you want to search. Log content options: logs, contentLogs, and localLogs.
<format>	The log formats to display, either rawFormat, or CSV.
<deviceName>	The device name you want to search logs from.
<logType>	Type of logs you want to search. Log type options: event, traffic, attack, antiVirus, webLogs, IM, email, content, history, generic, voIP, DLP, appCtrl, or netScan.
<searchCriteria>	The search criteria used to search logs. For example, vd-root.
<maxNumMatches>	The maximum number of matches to display from the search results.
<startIndex>	The start index of the matched logs.
<checkArchive>	This variable is not used. Always set the value to 0.
<DLPArchiveType>	The DLP archive type. DLP archive type options: web, email, ftp, IM, MMS, quarantine, or IPS.
<compression>	The compression type of the report that will be returned by this command.

The response will contain the logs that match the criteria specified in the request.

Example request:

```
<soapenv:Header/>
```

```
<soapenv:Body>
   <r20:searchFazLog>
      <servicePass>
         <userID>admin</userID>
         <password></password>
      </servicePass>
      <adom>root</adom>
      <content>logs</content>
      <format>rawFormat</format>
      <deviceName></deviceName>
      <logType>traffic</logType>
      <searchCriteria>?</searchCriteria>
      <maxNumMatches>5</maxNumMatches>
      <startIndex>1</startIndex>
      <checkArchive>0</checkArchive>
      <DLPArchiveType>web</DLPArchiveType>
      <compression>tar</compression>
   </r20:searchFazLog>
</soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:searchFazLogResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>searchFazLog successfully</errorMsg>
      </errorMsg>
      <totalResultsFound>20</totalResultsFound>
      <matchesReturned>2</matchesReturned>
      <startIndex>1</startIndex>
      <logs>
         <data>
            <logEntry>date=2015-10-07 time=10:10:28 itime=1444237829 logver=52 logid=13
                type=traffic subtype=forward level=notice vd=root devid=FG200B3910601180
                action=close trandisp=snat srcip=192.168.1.86 srcname=192.168.1.86
                srcport=47771 dstip=96.45.33.97 dstname=96.45.33.97 dstport=443
                service=HTTPS proto=6 duration=5 policyid=2 sentbyte=3312 rcvdbyte=4073
                sentpkt=11 rcvdpkt=12 srcintf=port11 dstintf=port9 sessionid=118281674
                app=HTTPS appcat=Not.Scanned transip=172.16.96.6 transport=47771
                dstcountry="United States" srccountry=Reserved</logEntry>
         </data>
         <data>
            <logEntry>date=2015-10-07 time=10:10:28 itime=1444237829 logver=52 logid=13
                type=traffic subtype=forward level=notice vd=root devid=FG200B3910601180
                action=close trandisp=snat srcip=192.168.1.86 srcname=192.168.1.86
                srcport=47423 dstip=208.91.112.136 dstname=forticlient.fortinet.net
                dstport=443 service=HTTPS proto=6 duration=5 policyid=2 sentbyte=3312
                rcvdbyte=4009 sentpkt=11 rcvdpkt=11 srcintf=port11 dstintf=port9
                sessionid=118281673 app=HTTPS appcat=Not.Scanned transip=172.16.96.6
                transport=47423 dstcountry="United States" srccountry=Reserved</logEntry>
         </data>
      </logs>
   </ns3:searchFazLogResponse>
</SOAP-ENV:Body>
```

Request Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • -101: Invalid username, password, or ADOM. Cannot get device name. Cannot get search criteria. Incorrect DLP archive type. • -102: Cannot find device name on system. • -104: Cannot find logs with criteria. • -106: Not enough memory.
<errorMsg>	
<totalResultsFound>	The total number of logs found.
<matchesReturned>	The total number of logs which matched the search criteria.
<startIndex>	The start index in the request.
<logs>	Log data will be displayed under this element.
<logEntry>	Displays log data.

setFazConfig

Use this request to set the FortiAnalyzer configuration. You can set either partial or full configuration.

Request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:setFazConfig>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <!--type: string-->
         <userID>?</userID>
         <!--Optional:-->
         <!--type: string-->
         <password>?</password>
      </servicePass>
      <!--Optional:-->
      <!--type: string-->
      <adom>?</adom>
      <!--Optional:-->
      <!--type: string-->
      <config>?</config>
   </r20:setFazConfig>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<adom>	The ADOMs for which you want to set the configuration.
<config>	The configuration content to be sent.

The response indicates if the request was successful or if it failed. In the case of a failure, the details of the failure, including the line number, are provided.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:setFazConfig>
      <servicePass>
         <userID>admin</userID>
         <password></password>
      </servicePass>
      <adom>root</adom>
      <config>
         config system interface
            edit "port2"
               set ip 1.1.1.254 255.255.255.0
               set allowaccess ping https http snmp ssh telnet webservice
         end
      </config>
   </r20:setFazConfig>
</soapenv:Body>
```

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:setFazConfigResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>setFazConfig successfully</errorMsg>
      </errorMsg>
   </ns3:setFazConfigResponse>
</SOAP-ENV:Body>
```

Request Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.

Request Field	Description
<errorCode>	Error code and message details: • -101: Invalid username, password, or ADOM. Cannot get configuration value. • -104: Cannot set configuration.
<errorMsg>	
<errorLineNumber>	The line number where the error occurs.

FORTINET®

High Performance Network Security